

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

information associated with the Apple IDs and Apple
iCloud accounts, more fully described in Attachment A,
that is stored at premises controlled by Apple.Case No. 19-MJ-1246

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See Attachment B.

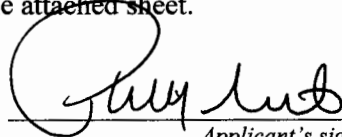
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of 18 U.S.C. § 1951, 18 U.S.C. § 924(c)(1)(A)(ii), 18 U.S.C. §§ 922(g)(1) and 924(a)(2), 18 U.S.C. § 4, 18 U.S.C. §§ 922(d)(1), 924(a)(2), 18 U.S.C. § 1519, and 18 U.S.C. § 1001.

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

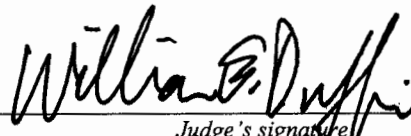


Applicant's signature

Philip Simment (Detective)

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 3/27/19


Judge's signature

City and State: Milwaukee, Wisconsin

Case 2:19-mj-01246-WED Filed 06/24/19 Page 1 of 31 Document 1

William E. Duffin, U.S. Magistrate Judge

Printed Name and Title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Detective Phillip Simmert, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the Apple IDs and Apple iCloud accounts associated with the following information, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014:

- a) Apple ID wjohnson8710@gmail.com
- b) Apple ID mz.lena9008@gmail.com
- c) Apple ID shakelaglover@gmail.com
- d) Apple ID mikemarrero2004@gmail.com
- e) Name: William Andrew Johnson
 - i) Date of birth: 01-25-1987
 - ii) Phones: 414-578-0901; 414-375-6569
 - iii) Address: 5471 North 42nd Street, Milwaukee, Wisconsin 53209
 - iv) Email: wjohnson8710@gmail.com
- f) Name: Lena Khiara Johnson
 - i) Date of birth: 09-04-1990
 - ii) Phone: 414-578-0046
 - iii) Address: 5471 North 42nd Street, Milwaukee, Wisconsin 53209
 - iv) Emails: lenakj9008@gmail.com; mz.lena9008@gmail.com

- g) Name: Shakela T. Glover
 - i) Date of birth: 02-17-1992
 - ii) Phone: 414-306-1837
 - iii) Address: 2523 West Garfield Avenue, Milwaukee, Wisconsin 53205
 - iv) Email: shakelaglover@gmail.com
- h) Name: Zulymar Crespo
 - i) Date of birth: 11-07-1994
 - ii) Phone: 414-502-6260
 - iii) Address: 7726 West Becher Street, Apartment 13, West Allis, Wisconsin 53219
 - iv) Emails: zulymar.9859@gmail.com; latinabella10191@gmail.com

2. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

3. I am a detective with the Milwaukee Police Department's Criminal Investigations Bureau (CIB) – Robbery Division. I have been employed as a law enforcement officer for over seventeen years. I am currently assigned to the Federal Bureau of Investigation's Milwaukee Area Violent Crimes Task Force, where I regularly investigate violent crimes including bank robberies, commercial robberies, and carjackings.

4. I have received formal training in the investigation of violent crimes and extensive on-the-job training and experience in the investigation of robberies. I have regularly used subpoenas, warrants, and court orders during those investigation to obtain investigative leads and corroborative evidence. I have also regularly used electronic evidence, including evidence obtained from social media platforms, phone extractions, electronic communication service providers, and remote computing service providers to identify targets, subjects, and witnesses, to obtain evidence of intent, motive, manner, and means, and to identify the instrumentalities and proceeds of crime.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Throughout this affidavit, I refer to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom I have had regular contact about this investigation.

6. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of 18 U.S.C. § 1951 (interference with commerce by robbery and conspiracy to do the same), 18 U.S.C. § 924(c)(1)(A)(ii) (brandishing a firearm during a crime of violence), 18 U.S.C. §§ 922(g)(1) and 924(a)(2) (unlawful possession of a firearm by a prohibited person), 18 U.S.C. § 4 (misprision), 18 U.S.C. §§ 922(d)(1), 924(a)(2) (knowingly transferring a firearm to a prohibited person), 18 U.S.C. § 1519 (destruction of records), and 18 U.S.C. § 1001 (false statements to government agents), as described in Attachment B.

JURISDICTION

1. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

FIRST ROBBERY – DECEMBER 1, 2018

2. On December 1, 2018 at approximately 8:12 p.m., an armed robbery occurred at the T-Mobile store located at 138 East Capitol Drive in Milwaukee. The robbery was captured on surveillance video.

3. At approximately 8:10 p.m., the store manager, Lena Johnson, took out the garbage—something out of the ordinary. Before doing so, she put down the metal security shutters. This concealed the robbery from any passerbys. While outside, a black male wearing a black hooded sweatshirt, black pants, and black boots approached Lena. That person was later identified as William Johnson—Lena's husband. William, who wore a black mask to cover his face, was armed with a chrome-and-black semi-automatic handgun. William walked Lena back into the store with the gun pointed at her back.

4. After entering, William walked to the breakroom leaving Lena at the front entrance. Oddly, Lena did not flee or call the police. Instead, Lena shut the security shutters over the front door and slowly walked towards the breakroom without any sign of fear.

5. Two other employees were working at the time—Shakela Glover and Ariel Harsh. One of those employees, Harsh was counting money in the breakroom in advance of the store closing. Glover, who was wearing sunglasses inside, walked back with a second cash drawer, right before William entered. She looked up at the security camera for a moment and then calmly looked in William's direction.

6. Glover and Harsh then laid down on the floor, reportedly at the direction of William. William pointed the gun at both Glover and Harsh. Glover then picked up William's backpack and went to the two cash drawers—perfectly placed side-by-side on the desk.

7. Glover then started taking cash out of the drawer and placing them in William's backpack, while William gently pressed on her back. She continued to diligently grab the cash, while William walked back to the front. William then walked Lena back with a gun pointed at her back.

8. William initially pushed Lena to the floor, while Glover continued taking the cash. Lena then led William to the safe room, while Glover continued diligently grabbing cash, double checking to confirm that she did not leave any bills. Glover's body language was strange and inconsistent with that of a robbery victim.

9. In the safe room, Lena opened one safe. William then directed Glover to open another safe while William pointed the gun at her. Glover took the Apple iPhones one at a time and placed them in the backpack.

10. As William walked back through the breakroom with Harsh lying on the ground, William put his gun in his hoodie pocket and walked back through the store and out of the front entrance.

11. After William fled, Glover awkwardly ran to the front (as if pretending). Harsh got up, checked under the cash drawer, and looked for her phone. After checking their phones and texting, Lena, Glover, and Harsh then walked to the front of the store.

12. Glover was interviewed on scene by Detective Alexander Ayala of the Milwaukee Police Department. Glover stated in substance to Detective Ayala that she grabbed her cash drawer in advance of closing the store, at which point she observed her manager Lena coming inside the

store with a masked subject pointing a gun at her. Glover claimed that she ran to the back and that the robber ordered her to lay on the ground. The robber then threw the backpack at Glover and ordered her to put the money and cell phones into the backpack, which she did. Glover claimed that she got back on the ground, at which point the robber took the bag and left. When Glover heard the door bell and knew the robber had left, she jumped up, hit the alarm button, and called 911.

13. Shakela Glover provided the following pedigree information to case agents:

- a. Name: Shakela T. Glover
 - i. Date of birth: 02-17-1992
 - ii. Address: 2523 West Garfield Avenue, Milwaukee, Wisconsin 53205
 - iii. Phone: 414-306-1837.

14. Lena was also interviewed on scene by Police Officer Molly Krueger and Detective Kent Gordon. In substance, Lena claimed that she took out the trash before closing. While doing so, the robber approached, pointed a handgun at her, and stated "get back in the fucking store." She claimed that she felt the robber push a hard object in the middle of her back. Lena claimed that, after unlocking the front door to the store, she entered with the robber. Lena claimed that the robber ordered her to lock the door and that she complied, and that he ordered her to lay on the ground. Lena stated that the robber came back and asked her about the safes. Lena claimed that the robber ordered them to lay on the ground, and that they did so until he left, at which point she pushed the panic alarm and called 911. Lena also stated that she claimed that she thought that Glover had put the "bait phone" in the robber's backpack until she saw the bait phone was still on the shelf.

15. Lena Johnson provided the following pedigree information to case agents:

- a. Name: Lena Khiara Johnson

- i. Date of birth: 09-04-1990
- ii. Address: 5471 North 42nd Street, Milwaukee, Wisconsin 53209
- iii. Phone: 414-578-0046.

16. In total, William took approximately \$5,168.00 and nine Apple iPhone XS Max cell phones with a total value of approximately \$8,845.68.

SECOND ROBBERY – FEBRUARY 13, 2019

17. On February 13, 2019 at approximately 10:46 a.m., a second armed robbery occurred at the T-Mobile store located at 1438 East Brady Street in Milwaukee. That robbery was also captured on surveillance video.

18. Alissa Senda, an employee at the T-Mobile store, stated that she heard the front door open and observed a man, later identified as William Johnson, enter. He was wearing a dark hoodie with the hood up. William also had on a dark colored mask covering his face and was armed with a semiautomatic handgun, which he pointed at Senda and another coworker Zulymar Crespo.

19. Senda stated that William yelled “go to the back.” Frightened, Senda entered the PIN to open the back room. William then pointed the gun at Senda and Crespo and ordered them into the back room and told them to lay on the ground. Senda complied, but watched William filling his bag with cell phones. William, again, ordered them not to move and then fled the store.

20. Detective Tony Castro interviewed Crespo. Crespo stated in substance that she was working with Senda. Crespo claimed that the robber had come into the store. She observed the robber holding a handgun in his right hand. The robber pressed the gun to her back, ordered her to the back, and ordered them to enter the code to open the back office door. Senda complied

with the robber and entered the unlock code. Once inside the back room, the robber ordered them to get on the ground, at which point they both laid down. After the robber fled, they called the police.

21. Zulymar Crespo provided the following pedigree information to case agents:

- a. Name: Zulymar Crespo
 - i. Date of birth: 11-07-1994
 - ii. Address: 7726 West Becher Street, Apartment 13, West Allis, Wisconsin 53219
 - iii. Phone: 414-502-6260.

22. Surveillance video from that robbery shows William looking at the stock keeping unit (SKU) numbers, a machine-readable bar code for inventory tracking, on the cellphone boxes. As a matter of course, T-Mobile typically keeps a bait phone in the safe with the rest of the inventory. That bait phone has a specific SKU number. William took all of the cell phones in the safe except for the bait phone. Only an employee would know the SKU number for the bait phone.

23. In total, William took cell phones with a total value of approximately \$14,923.

INVESTIGATION

24. Case agents obtained surveillance video from that day showing William stepping out of the passenger side of a dark grey Chevrolet Tahoe with Wisconsin license plate 951-YFB right before the robbery. That license plate and vehicle is registered to William Johnson at 5471 North 42nd Street in Milwaukee, Wisconsin—an address also listed for William's wife Lena.

25. A review of law enforcement records shows that Lena Johnson was stopped in that Chevrolet Tahoe on November 18, 2017 and that Lena Johnson received a citation while driving that vehicle on March 28, 2018.

26. Case agents also obtained surveillance video from a Milwaukee County Transit System bus, which captured the Johnsons' Chevrolet Tahoe driving westwards on Brady Street after the robbery.

27. Case agents identified several distinguishing features about the Johnsons' Chevrolet Tahoe— a distinctive after-market rectangular exhaust tip extending from the right rear quarter panel, a center cap on the black steel rim of the right rear wheel, aluminum rims on the remaining wheels, and after-market window exhaust vents.

28. On February 17, 2019 at approximately 9:30 a.m., Detective Simmert observed the Johnsons' Chevrolet Tahoe parked in the driveway of 5471 North 42nd Street. Upon knocking on the door, Lena answered and allowed the police to enter their residence. Lena stated that she and her husband reside at that address and that she was the sole driver of the Chevrolet Tahoe on Wednesday, February 13, 2019. She claimed that her phone would not place her anywhere near Brady Street at the time of the robbery and that no text messages on her phone would implicate her in the robberies. Lena also provided consent to search her residence. During the search, case agents located shoes similar to the ones used during the Brady Street robbery and gloves, face mask, and blue jeans similar to those used in the robbery. They also recovered Lena's Apple iPhone and William's Apple iPhone.

29. A search of the Tahoe revealed a silver-over-black Smith & Wesson .40 caliber handgun with a laser sight with 12 hollow-point bullets in the magazine and 1 in the chamber, which matched the one used in the robberies. Case agents recovered that gun from between the driver's seat and front console, along with registration documents listing the vehicle to William Johnson.

30. William Johnson was previously adjudicated a delinquent for the felony offense of Armed Robbery, in violation of Wisconsin Statute 943.32, in Milwaukee County Juvenile Court Case No. 2003JV1362 on December 26, 2003. That adjudication remains of record and unreversed.

31. During an interview with Detective David Anderson, William Johnson admitted that he committed the robberies at the T-Mobile stores on December 1, 2018 and February 13, 2019.

32. With respect to the robbery on December 1, 2018, William implicated his wife and Shakela Glover. William claimed that he received a call from Lena on the day of the robbery. Lena indicated that she and Glover thought that William should rob the T-Mobile store and that the store had about \$6,000 in cash. William indicated that he could hear Glover saying that the robbery had to “make sense” and “look like it is random.” William indicated that they planned for Lena or Glover to take out the trash out, at which point William would push them back in the store with his gun. William indicated that Lena wanted him to point the gun at her to make the robbery look real. He stated that, after the robbery, they split the money three ways, with William, Lena, and Glover each taking \$1,700, at the Johnsons’ house. Glover did not want the cell phones. William later sold the cell phones at a corner store located at North 39th Street and West Burleigh Street in Milwaukee. Case agents later identified this corner store as Hakote Food Mart, located at 3830 West Burleigh Street.

33. With respect to the robbery on February 13, 2019, William implicated his wife Lena and Zulymar Crespo. He indicated that his wife received a call from Crespo informing them of the best time to commit the robbery and providing information about the bait phone. William also stated that his wife Lena and son were with him during the robbery. Lena drove the Chevrolet Tahoe and dropped him off near the store. William admitted that he had the gun,

which Lena had purchased for him, at the time of the robbery and that the gun was loaded. Lena waited in the Tahoe on the side of the store and then drove during the getaway. After the robbery, they drove to the Hakote Food Mart to sell the phones.

34. William Johnson provided the following pedigree information to case agents:

- a. Name: William Andrew Johnson
 - i. Date of birth: 01-25-1987
 - ii. Phone: 414-375-6569; 414-578-0901
 - iii. Address: 5471 North 42nd Street, Milwaukee, Wisconsin 53209

35. Case agents obtained surveillance video from the Hakote Food Mart from February 13, 2019, which shows William step out of the passenger side of the Tahoe, walk into the store with the bag shortly after, hand the bag to a store employee, leave, and then reenter the passenger side of the Tahoe—less than an hour after the robbery.

36. During interviews with case agents, Lena denied any involvement in the robberies and denied that her husband was involved in the robberies. She again provided a phone number of 414-578-0046. Lena stated that she is married to and has two children with William Johnson. She stated that she purchased the gun recovered from the Chevrolet Tahoe as a gift for her husband William Johnson about four years ago.

37. During interviews with case agents, Shakela Glover also denied any involvement in the robbery and, again, recounted her description of the robbery on December 1, 2018. That said, Glover admitted that she is close with Lena and indicated that they call each other cousins, even though they are not related by blood.

38. Case agents obtained surveillance video and transaction records from the Walmart store located at 401 East Capitol Drive in Milwaukee. That surveillance video shows the Johnsons' Chevrolet Tahoe pull in front of the entrance to the Walmart and drop off Lena. At about 10:22

a.m. on February 13, 2019, the surveillance video and transaction records show Lena purchasing scissors, Gorilla tape, and a sweatshirt at the register, before voiding the purchase of the scissors and Gorilla tape. That surveillance video also shows Lena then leaving the Walmart. The hooded sweatshirt that Lena purchased at Walmart—minutes before the robbery—is consistent with the hooded sweatshirt that William wore during the robbery on February 13, 2019, as captured by surveillance video.

39. On February 19, 2019, I interviewed Zulymar Crespo. She stated that she received a phone call from Lena the night before the robbery asking what time Crespo would work, what time Dunbar Armored security comes to the store, and if Crespo still had the codes.¹ Apparently, Lena indicated that the robbery would happen the next day, but not how the robbery would happen. Lena indicated that she would pay Crespo \$200 after the robbery, but that Crespo never received the proceeds and never had any intention of taking the money. Crespo denied telling Lena anything about the bait phone.

PHONE EXTRACTIONS

40. Case agents forensically extracted the data from William Johnson's Apple iPhone. The extraction report indicates that William's phone has a call number of 414-578-0901 and Apple ID wjohnson8710@gmail.com.

¹ This information is consistent with the call history on Lena Johnson's Apple iPhone, which indicates that Lena placed an outgoing call to Zulymar Crespo at 414-502-6260 on February 12, 2019 at 10:09 p.m. That call only lasted four seconds. However, Crespo and Lena had another call at 10:09 p.m., which lasted 3 minutes and 53 seconds, and a third call at 10:13 p.m., which lasted 2 minutes and 10 seconds.

41. Immediately after the robbery on December 1, 2018, William sent and received the following text messages directly after the robbery on December 1, 2018:

28157	Instant Messages	Incoming			12/1/2018 21:13(UTC-6)	From: +14145303219 Z	Gone let ya boy hold a dollar or two if u can stand it Source Extraction: File System
28158	SMS Messages	Outgoing			12/1/2018 21:15(UTC-6)	To: +14145303219 Z	Gotta wait for the wife to make it here to bust it down. But I'll see what I can do bro Source Extraction: File System, Logical
28159	Instant Messages				12/1/2018 21:21(UTC-6)	From: +14145303219 Z	Fa sho Source Extraction: Logical

42. William and Lena also exchanged text messages implicating Lena, Zulymar Crespo, and Audreanna Watson, who was charged in an unrelated burglary, in a prepaid scam at T-Mobile. In those messages, William asks whether Crespo or Watson “ratted” on Lena, to which Lena responds: “They didn’t snitch.” Lena indicates that the prepaid scam was “Bigg!!” and expresses concern that T-Mobile may find “the old deposit shit.”

43. In a different string of text messages, William contacts another person about buying a laser “beam” for his “Smith & Wesson 40.” Some of these messages were sent and received as Apple iMessages. After these text messages were sent, officers recovered a Smith & Wesson .40 caliber handgun with a laser sight from William’s Chevrolet Tahoe.

44. Case agents also forensically extracted the data from Lena’s Apple iPhone. The extraction report confirms that the assigned call number for Lena’s phone is 414-578-0046. The Owner ID listed on the phone was “Lena’s iPhone” with an Apple ID of mz.lena9008@gmail.com.

45. On November 30, 2018—the day before the first robbery, Lena sent a text message to 414-524-9229, listed as “Rihanna,”² with a photograph of a “Corrective Action” issued by

² “Rihanna” may refer to Audreanna Watson, who was charged with Burglary of a Building or Dwelling, in violation of Wisconsin Statute 943.10(1m)(a), in Milwaukee County Case No. 2019CF000520, for a burglary at the T-Mobile store located at 1438 East Brady Street in Milwaukee.

Wireless Vision, the corporate name for T-Mobile's retail locations, providing a final written notice to Lena about two internal policy violations. After that message, Rihanna responds: "Yeah it's time to go. Gotta rob them on the way out too.," which Lena emphasized. Rihanna later said: "Steal all the deposits," to which Lena responds: "I am!! And I'm sticking to my plan of quitting and telling them it's bc my safety was at risk.." Rihanna suggested: "Pin it on Lloyd lmao," which Lena emphasized and said: "It's gone look like he did it anyway.." Lena and Rihanna continue to discuss pinning the scheme on "Lloyd."

46. Lena also sent the photograph of the "Corrective Action" to William.

47. That evening before the robbery at 5:56 p.m., Lena tells Rihanna: "Ima talk to Drew and put shit in motion..Lbvs. I JUST CANT BELIEVE I WORKED FOR THIS BITCH ASS COMPANY FOR 7 YEARS, NEVER BEEN WROTE UP AND THEN THIS NIGGA COME FOR FIVE MINUTES AND IM ON A FINAL!!! I'm mad now.. I wanna rob him too!!!"

48. After the robbery on December 1, 2018 concluded, Lena exchanged messages with 414-306-1837, listed in her contacts as "Shakela Glover." At about 11:18 p.m., Glover asked, "House?," to which Lena responds: "Yea." This is consistent with William's statement that Glover met at the Johnsons' house to split the proceeds of the robbery.

49. In the early morning hours after the robbery, Lena asked Glover if she had called Lloyd. Glover responded: "Yeah. I asked him did he set us up cause he was joking about it and you was scared and would probably talk to him tomorrow cause you just wanted to be with family.....he think I think he did it and I do." Lena responded: "I do too!!!" Lena forwarded this text string to Rihanna with a winking smiley face emoji.

50. On February 12, 2019 at 10:09 p.m.—the night before the second robbery, the call history on Lena Johnson's Apple iPhone indicates that Lena placed an outgoing call to Zulymar

Crespo at 414-502-6260. That call only lasted four seconds. However, Crespo and Lena had another call at 10:09 p.m., which lasted 3 minutes and 53 seconds, and a third call at 10:13 p.m., which lasted 2 minutes and 10 seconds.

51. Around 10:00 a.m. on February 13, 2019, Lena exchanged a text message with Rhianna at 414-524-9229 stating: "He got on a recognizable ass Adidas hoodie, no hat, no gloves, just a face mask.. Like fam...ARE YOU TRYING TI GET CAUGHT!? Didn't put tape over the gun." This message was sent shortly before Lena was captured at Walmart purchasing a hooded sweatshirt and attempting to purchase scissors and Gorilla tape. Lena goes on: "And I feel like once the pic circulates, Jerron ass gone be the one to recognize him.. We on our way now." At 10:46 a.m., Lena sent an update: "I just let him out.. Fam! The adrenaline rush off this shit is crazy!" The second robbery happened at about 10:46 a.m.

52. Later that evening, Lena continued to text Rihanna stating that Lena contacted Crespo on Snapchat, because she wanted to know about the preliminary investigation of the second robbery. Anxious about Crespo's lack of a response, Lena texted Rhianna stating: "She probably got ptsd and shit.. Drew put the barrel on her back and shit.." I know that William Johnson's middle name is Andrew.

53. The call history on Lena's phone for February 13, 2019 also indicates that she spoke with William at 5:57 p.m. for 1 minute and 15 seconds, Crespo at 6:49 p.m. for 6 minutes and 18 seconds, Glover at 6:58 p.m. for 14 minutes and 24 seconds, Crespo at 7:13 p.m. for 6 minutes and 17 seconds, and with William at 7:39 p.m. for 48 seconds.

54. At about 7:00 p.m., Lena texts William at 414-578-0901 and says: "Zuly said they think it's the same guy who did East Cap.." To which he responds, "That's good and bad." Lena responds: "Why you say that??" Responding to Rihanna, Lena recounts Crespo's description of

the surveillance video: “But she did say the footage was dark af and he kept his head down so you can’t see shit except his shoes (which was some old ass foams that he threw away once we left) and his gun from when he flashed it.”

55. The GPS location information and wireless connectivity information indicate that Lena Johnson was at her residence located at 5471 North 42nd Street at 11:37 a.m. shortly after the robbery.

56. Case agents also forensically extracted the data from Shakela Glover’s Apple iPhone. That extraction report confirms that the phone number associated with her phone is 414-306-1837 and her Apple ID is shakelaglover@gmail.com. Glover has several texts with Lena Johnson at the phone number 414-578-0046. There were numerous texts exchanged with Lena contained in the phone’s extracted data, but the only calls exchanged were on February 8, February 9, February 14, and February 17, 2019. The call history prior this appears to have been deleted. The extracted data has no search history between October 5, 2018 and December 23, 2018, even though Glover otherwise conducted searches almost every day. It appears that the search history for those dates was deleted.

57. On or about February 19, 2019, Glover exchanged text messages with 414-524-9229, a person listed as “Shahd”—the same number listed for “Rihanna” in Lena’s phone. Rihanna texted Glover saying: “But the Zuly thing really blew me. Because she got fired and arrested and jerron said she must’ve name dropped because why would they also arrest Drew.” Glover then responds: “Right, She still gone get charged because she was party to the crime.,” referring to Crespo.

58. As a part of this investigation, I monitored Glover’s jail calls. On February 25, 2019, Glover placed a phone call to her mother Felicia Jackson at 414-419-7540. Glover instructed

her mother to contact T-Mobile and delete her iCloud account. Glover gave specific instructions to her that T-Mobile will ask for an authentication ID and send a code to the phone. Glover provided her mother with a personal identification number (PIN) of 9886 and an Apple iCloud password. Glover also instructed her mother to change the SIM card on the phone and to log on to the computer and delete all devices. Glover's directives to her mother evinced not only a consciousness of guilt, but an attempt to destroy records or evidence relating to this investigation.

59. Finally, case agents extracted the data from Zulymar Crespo's Apple iPhone. That extraction report confirms that the phone number associated with her phone is 414-502-6260. The Apple ID listed in the extraction report is mikemarrero2004@gmail.com and the Facebook account is latinabella10191@gmail.com.

60. That extraction report also indicates that Crespo sent a message to 414-520-7271 on or about December 14, 2018 stating: "Dawg I just got off the phone with Lena," with a smack-in-the-face emoji. Crespo continues to express some concern about the fraud investigations at the Brady Street location.

PRESERVATION LETTERS

61. Assistant United States Attorney Philip T. Kovoov sent a preservation letter to Apple, Inc. requesting preservation of all stored communications, records, and other evidence relating to the Apple ID and Apple iCloud account for Lena Johnson on March 16, 2019.

62. Special Agent David Kowalski of the Federal Bureau of Investigation sent a preservation letter to Apple, Inc. requesting preservation of all stored communications, records, and other evidence relating to the Apple ID and Apple iCloud accounts for William Johnson, Shakela Glover, Zulymar Crespo, Ariel Harsh, Alissa Senda, and Audreanna Watson on March 18, 2019.

INFORMATION REGARDING APPLE ID AND iCloud³

63. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

64. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

³ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or

through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

65. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

66. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

67. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the

length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

68. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

69. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be

captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

70. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

71. This is a complex investigation of two robberies involving multiple targets, subjects, and witnesses at two locations on two dates. Many of those people work for wireless telephone providers and are, presumably, familiar with cellular device technology. The evidence indicates that the targets, subjects, and witnesses communicated regularly using Apple iPhones,

that they were engaged in an ongoing criminal scheme, and that the targets and subjects actively took steps to conceal their activities. At the very least, the requested information will provide corroboration of the evidence described-above, including but not limited to the information contained in the extraction reports, and provide another method for authenticating that information. In light of the apparent destruction of evidence and attempts to destroy evidence, the requested information will likely contain evidence that has been deleted, altered, or destroyed from those cellular devices.

72. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

73. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

74. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account—and when that user had controlled of the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example,

subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

75. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). The evidence outlined above already indicates that the targets and subjects communicated regularly about the plan to commit these robberies and attempts to conceal evidence from law enforcement.

76. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

77. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

78. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

79. Based on the forgoing, I request that the Court issue the proposed search warrant.

80. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”),

Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from September 1, 2018 to March 26, 2019, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from September 1, 2018 to March 26, 2019, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud

Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1951 (interference with commerce by robbery and conspiracy to do the same), 18 U.S.C. § 924(c)(1)(A)(ii) (brandishing a firearm during a crime of violence), 18 U.S.C. §§ 922(g)(1) and 924(a)(2) (unlawful possession of a firearm by a prohibited person), 18 U.S.C. § 4 (misprision), 18 U.S.C. §§ 922(d)(1), 924(a)(2) (knowingly transferring a firearm to a prohibited person), 18 U.S.C. § 1519 (destruction of records), and 18 U.S.C. § 1001 (false statements to government agents) involving William Johnson, Lena Johnson, Shakela Glover, Zulymar Crespo, Ariel Harsh, or Alissa Senda since September 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Robbery;
- b. A conspiracy to commit robbery;
- c. Brandishing a firearm during a crime of violence;
- d. Unlawful possession of a firearm by a prohibited person;
- e. Knowingly transferring a firearm to a prohibited person;
- f. Destruction of records or evidence relating to a federal investigation;
- g. False statements to government agents;
- h. Communications between William Johnson, Lena Johnson, Shakela Glover, Zulymar Crespo, Ariel Harsh, or Alissa Senda;

- i. Information about the affiliations, relations, or associations between William Johnson, Lena Johnson, Shakela Glover, Zulymar Crespo, Ariel Harsh, or Alissa Senda;
- j. Information about the theft, taking, transfer, sale, or disposition of cell phones;
- k. Information about the location or whereabouts of William Johnson, Lena Johnson, Shakela Glover, Zulymar Crespo, Ariel Harsh, or Alissa Senda around the times of the violations described above;
- l. Preparatory steps taken in furtherance of the scheme or conspiracy;
- m. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- n. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- o. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- p. Evidence indicating the subscriber's state of mind as it relates to the crimes under investigation; and
- q. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.